

AMENDMENT OF THE CLAIMS:

Please amend Claims 13, 19, 20 and 22-24 as follows:

Claims 1-12 (canceled)

Claim 13 (currently amended): A method of reducing payments risk, liquidity risk, and systemic risk associated with payments-based transactions, in a system supporting a plurality of third party host applications, a plurality of user host applications, and a plurality of payment bank host applications running on a communications network,

wherein said plurality of user host applications are supported over said communications network for use by a plurality of users active in payments-based transactions,

wherein said plurality of third party host applications are supported over said communications network for use by plurality of third parties active in payments-based transactions,

wherein said plurality of payment bank host applications are supported over said communications network for use by a plurality of payment banks operating a plurality of domestic payment systems, and

wherein each said payment bank host application has a filter process module for processing payments instructions, said method comprising the steps:

(a) said third parties sending counterparty payments risk data associated with a plurality of payments-based transactions, to said user host applications;

(b) said users sending counterparty payments risk data on behalf of themselves and said third parties to said system, wherein said payments risk data specifies transaction parameters selected from the group consisting of

(i) said ~~user-associated~~ user associated with each said payments-based transaction,

(ii) said third party associated with each said payments-based transaction,

(iii) said payment bank associated with each said payments-based transaction,

(iv) an intermediary(ies) in the chain of accounts leading to the counterparty or ultimate payment beneficiary,

(v) a counterparty associated with each said payments-based transaction,

- (vi) ~~a~~ a currency associated with each said payments-based transaction,
- (vii) a payment type associated with each said payments-based transaction,
- (viii) a Transaction Reference Number unique to each ~~payment~~ payments-based transaction, and
- (ix) a clean payment limit associated with each said payments-based transaction;
- (c) said system analyzing the payments risk data associated with each said payments-based transaction and decomposing said payments risk data into files for transfer to said payment bank host applications for making payments on behalf of said users in a plurality of currencies;
- (d) said system transmitting said payments risk data, associated with each said payments-based transaction, to said payment bank host applications, using application-to-application automated interfaces; and
- (e) each said payment bank host application applying said payments risk data, as input parameters, to said filter process module for automated evaluation of payments instructions in respect of accounts of said users such that payments instructions breaching said input parameters to said filter process module are rejected back to a payments processing queue for later re-evaluation in the absence of an override instruction.

Claim 14 (original): The method of claim 13, wherein each third party, user and payment bank sending payments risk data can also generate and receive payments-related notifications, inquiries, messages and reports via their respective host applications.

Claim 15 (original): The method of claim 13, wherein said filter process module within each said payment bank host application cooperates with payments processing with a domestic payment system operated by said payment bank, such that payments instructions are filtered by said filter process module for compliance with suspend instructions, override instructions and payment risk parameters.

Claim 16 (original): The method in claim 14, wherein each third party and user can request and receive reports from a plurality of said payment banks acting on their behalf.

Claim 17 (original): The method of claim 13, wherein each said payment bank host application capable of calculating the available balance for counterparty payments through incorporation of data interchange with existing payments confirmation services and monitoring elapsed time.

Claim 18 (original): The method of claim 14, wherein each payment bank host application can generate a notification to the payment bank and user and/or third party in the event that a counterparty fails to make expected payments for a pre-determined period of elapsed time and detail payments which have failed to pass the filter process according to their transaction reference numbers.

Claim 19 (currently amended): The method of claim 18, wherein each third party of user receiving notification of a counterparty payment failure may instruct payment bank ~~suspension~~ ~~of to suspend~~ further payments to said counterparty or instruct ~~override~~ the overriding of the filter process to allow individual identified payments to proceed or allow payments to specified counterparties or intermediaries.

Claim 20 (currently amended): The method of claim 17, wherein each payment bank host application ~~will~~ automatically ~~incorporate~~ incorporates a suspension of all further payments to a counterparty on receipt of a notification to do so via implementation as a trigger in the filter process module and ~~incorporate~~ incorporates overrides as instructed.

Claim 21 (original): The method of claim 13, wherein each payment bank and user are subjected to digital certification to establish their access authority and usage constraints, and wherein data transmissions are encrypted for security purposes.

Claim 22 (currently amended): The method of claim 13, wherein third party, user and payment bank host applications are human-accessible by a browser interface and machine-accessible by incorporation and translation of electronic data interchange (EDI) formats.

Claim 23 (currently amended): The method of claim 13, wherein third parties and users can flexibly identify counterparties by means of aggregating identifiers unique to individual corporate or organizational entities, thereby creating ~~thereby~~ synthetic counterparties composed of entities deemed to share correlation in payment risk assessment.

Claim 24 (currently amended): The method of claim 13, wherein said system further comprises a core system host application for recording various type of information, including identification of said users, identification of said third parties, identification of said payment banks, identification of said counterparties, identification of currencies, specification of the clean payment limit (debit cap), any override instructions, and payment type identification, including alternative payment channels, if any.

Claims 25-56 (canceled)